Express Mail Label No.: E[illegible]7475247US
Dat Mailed: December 10, 1999

UNITED STATES PATENT APPLICATION FOR GRANT OF LETTERS PATENT

MOHAMMAD PEYRAVIAN
ALLEN ROGINSKY
NEVENKO ZUNIC
STEPHEN M. MATYAS, JR.
INVENTORS

TIME STAMPING METHOD USING TIME-BASED SIGNATURE KEY

C ATS & BENNETT, P.L.L.C.
P.O. Box 5
Raleigh, NC 27602
(919) 854-1844

TIME STAMPING METHOD USING TIME-BASED SIGNATURE KEY

BACKGROUND OF THE INVENTION

The present invention relates generally to cryptographic protocols and, more particularly, to a time-stamping protocol for time-stamping digital documents.

There are times when it is desirable to prove the existence of a document as of a particular date. For example, patent disputes concerning the inventorship of an invention often turn on who is able to produce corroborating documentary evidence dating their conception of the invention. A common procedure for dating records is to keep the records in a daily journal or notebook with each page sequentially numbered and dated. Another procedure for dating a record is to have the record witnessed by an uninterested or trusted party that can attest to the existence of the document. The increasing use of computers, however, makes these time-stamping methods obsolete. It is relatively easy to change the date-stamp added to a document by the computer when the document was created. Further, while it is difficult to alter a paper document without leaving some signs of tampering, digital records can be easily altered or revised without leaving any evidence of tampering. Therefore, people are less likely to trust a digital document than a paper document that has been time-stamped using conventional time-stamping procedures.

To be trusted, a time-stamping procedure for digital documents should meet the following criteria:

1. The data itself must be time-stamped, without any regard to the physical medium on which it resides.

2. It must be impossible to change a single bit of the data without that change being apparent.

3. It must be impossible to timestamp a document with a date and time different than the current date and time.

One method for time-stamping a digital document would be to archive the document with a trusted escrow agent. In this case, the document originator sends a copy of the digital document to a trusted escrow agent. The escrow agent records the date and time that the document was received and retains a copy in his archives. Later, if a dispute arises over the date of the document, the document originator can contact the escrow agent who produces his copy of the document and verifies that it was received on a particular date. This time-stamping procedure has a number of drawbacks. First, the document originator must disclose the contents of the document to the escrow agent. Also, large documents take a relatively long period of time to transmit to the escrow agent and they require a large amount of data storage.

An improvement of the escrow procedure is to use a hash of the document. Instead of sending the document to the escrow agent, the document originator hashes the document using a one-way hash algorithm and sends the generated hash value to the escrow agent. The escrow agent stores the hash

value along with the date and time that it was received in his archives. Later the document originator can use the services of the escrow agent to prove the existence of the document as of a particular date. The disputed document can be hashed and the resulting hash value can be compared to the hash value stored by the escrow agent in his archives for equality. If the hash values are equal, the document is presumed to be in existence as of the date associated with the stored hash value. One advantage of this method is that the document originator does not need to disclose the contents of the document to the escrow agent.

The need to escrow the document or hash value can be eliminated by having a time stamping authority generate a certified time stamp receipt using a cryptographic signature scheme as taught in U.S. Pat. No. Re. 34,954 to Haber et al. and Fischer, U.S. Patent No. 5,001,752. In this case, the document originator hashes the document and transmits the hash value to the time stamping authority. The time stamping authority appends the current date and time to the hash value to create a time stamp receipt and digitally signs the time stamp receipt with a private signature key. The time stamping authority's public verification key is distributed and available to anyone interested in validating a time stamp receipt created by time stamping authority. The public verification key is typically stored in a public key certificate signed by a Certification Authority so that anyone desiring to validate the time stamp receipt with the public key can have confidence in the authenticity of the key.

Another approach to time stamping documents is disclosed in PCT WO 99/16209 entitled Method and System For Transient Key Digital Time Stamps. In this application, time stamp receipts are signed by the time stamping authority using transient, time-related keys. The time-stamping authority periodically generates a signature generation key, which is valid for a predetermined interval of time. Documents received during the specified time interval are signed using the key corresponding to that interval. At the end of the interval, a new key is generated for the next interval and the previously used key is discarded. In this manner, a new signature generation key is generated at a predetermined interval of time. The public verification key associated with each private signature generation key is saved for future authentication of the time stamp receipt.

SUMMARY OF THE INVENTION

The present invention is a time-stamping protocol for time-stamping digital documents so that the date of the document can be verified. The method presumes the existence of a trusted agent referred to herein as the time-stamping authority (TSA). The TSA has a time-based signature key that the TSA uses to sign time stamp receipts. The signature key is associated with a fixed time reference. According to the present invention, a requestor sends a document to be certified or other identifying data associated with the document to a time-stamping authority TSA. The TSA creates a time stamp receipt by computing a time difference between the time reference associated with the signature key and the time the document was received. The time difference is

appended to the identifying data received by the TSA to create a time stamp receipt and the receipt is then signed by the TSA and transmitted to the requestor.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a flow diagram illustrating the time stamping method embodiment of the time stamping method of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 is a flow diagram illustrating the general process of time-stamping a document according to the present invention. A document D is created at step 100. The document D is presumed to be in digital form and may comprise any alphanumeric, audio, or graphic presentation of any length. The document D may optionally be hashed at step 102 using a one-way hashing function. A hash function is a function that takes a variable length input string, called a pre-image, and converts it to a fixed-length string, called a hash value, denoted H. The pre-image in this case is the document D or selected portions thereof. A one-way hash function operates in only one direction. While, it is easy to compute a hash value from the pre-image, it is computationally impractical to find a pre-image that hashes to a given hash value. Thus, it is practically impossible to recover the pre-image given the hash value and knowledge of the hash algorithm. Another feature of a hashing function is that it is difficult to find any two pre-images that hash to the same value.

There are several advantages to sending a hash value H produced on document D instead of the document D itself. First, the hash value H improves security by functioning as a fingerprint of the document D. Changing a single bit in the document D will result in an entirely different hash value making it easy to detect efforts to modify a document D or hash value H. Second, the hash value H greatly reduces the amount of data that must be transmitted to the TSA. This factor can be important where the available bandwidth is limited. Third, by sending a hash value H in place of the document D, the content of the document D does not need to be disclosed to the TSA.

Any known hashing function, such as the SHA-1, MD5, and RIPEMD-160, can be used in the present invention. For the remaining description of the time stamping protocol, it will be assumed that the document D has been hashed and that the hash value H has been sent to the TSA in lieu of the document D. It is understood, however, that one can practice the invention by substituting D, selected portions of document D, or some other function of D in place of the hash value H in the protocol.

The hash value H generated on document D or a selected portion thereof is transmitted to and received by the TSA at step 104 as part of a certification request. According to the present invention, the TSA has a time-based private signature key that the TSA uses to sign time stamp receipts R. The private signature key is part of a public and private key pair (K_P, K_{PR}). The private signature key K_{PR} is known only to the TSA. The public verification key K_P, is made available to the public so that anyone can verify or authenticate the TSA's

signature. The public key K_P can be stored in a certificate signed by a Certification Authority CA so that the TSA's public key can be validated and, hence, trusted by those using the public verification key K_P. The key pair has an associated time reference T_{REF} that is stored in the public key certificate along with the public verification key K_P. The time reference T_{REF} in the public key certificate can be established by the TSA when requesting the public key certificate or may be determined by the Certification Authority, or some completely independent means.

At step 106, the TSA computes a time difference ΔT between the time reference T_{REF} recorded in the public key certificate and the current time T. The current time T is generated by a trusted clock controlled by the TSA, or alternatively, is obtained by the TSA from a trusted source. The TSA creates a time stamp receipt R at step 108 using the computed time difference ΔT. The time stamp receipt R is generated by concatenating the hash value H with the computed time difference ΔT and optionally other data, such as the identification number ID of the requestor and a sequential record number SN. Requiring an identification number ID and sequential record number SN may improve security by making it more difficult to create counterfeit time stamp receipts. The time stamp receipt R would then comprise the string (H, ΔT, ID, SN). The TSA then signs the time stamp receipt at step 110 and transmits the time stamp receipt to the requestor at step 112. The signed time stamp is denoted sig(R).

In the event that a dispute arises concerning document D, the existence and substance and the document D as of a particular date can be proved by

means of the signed time stamp receipt sig(R). To verify the document D, the TSA's signature on the time stamp receipt, sig(R), is first verified using the TSA's public verification key K_P. Next, the disputed document D is verified against the hash value H contained in the time stamp receipt R. A hash value H is generated on the disputed document D and compared for equality to the hash value H contained in the signed time stamp receipt sig(R). The date or time of the document D is computed by adding the time difference ΔT contained in the signed time stamp receipt sig(R) to the time reference T_{REF} taken from the public key certificate.

The time-stamping procedures described herein may be implemented using general purpose programmable computers. A client program running on a user's computer could perform the steps of hashing documents, generating time stamp receipts, and transmitting time stamp receipts to the TSA. A server application running on a general purpose programmable computer controlled by the TSA could perform the steps of validating time stamp receipts, signing time stamp receipts, generating certificates, and transmitting signed time stamp receipts to users. It would also be possible to implement some or all of the steps in firmware, or in hard-wired logic.

The present invention may, of course, be carried out in other specific ways than those herein set forth without departing from the spirit and essential characteristics of the invention. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive, and all changes

coming within the meaning and equivalency range of the appended claims are intended to be embraced therein.